Amendments to the Claims

1. (Canceled).

2. (Currently Amended) ~~The method of Claim 1, wherein~~ A method of determining if a packet has a spoofed source Internet Protocol (IP) address, comprising:

evaluating a source media access control (MAC) address of the packet and the source IP address to determine if the source IP address of the packet has been bound to the source MAC address at a source device of the packet; and

~~determining that the source IP address of the packet is spoofed if the source IP address is not bound to the source MAC address further comprises~~ determining that the source IP address is spoofed if the source IP address is not bound to the source MAC address and the source MAC address is not associated with a gateway routing device,

wherein evaluating a source MAC address of the packet and the source IP address further comprises:

identifying an entry in an address resolution protocol (ARP) table corresponding to the source MAC address;

comparing an IP address of the identified entry to the source IP address to determine if the IP address of the identified entry corresponds to the source IP address;

identifying the source IP address as bound to the source MAC address at the source device if the IP address of the identified entry corresponds to the source IP address;

sending an ARP request to the source IP address if no entry in the ARP table is identified as corresponding to the source MAC address; and

incorporating an entry corresponding to the MAC address into the ARP table if a response is received to the ARP request.

3. (Previously Presented) The method of Claim 2, further comprising:

determining if the source MAC address is identified in an ARP table as a MAC address of a routing device to determine if the source MAC address is associated with a gateway routing device.

4. (Previously Presented) The method of Claim 3, wherein determining if the source MAC address is identified in an ARP table is preceded by:

determining if an IP address of a gateway routing device is to be added to a routing table;

sending an ARP request to the IP address of the gateway routing device;

receiving a response to the ARP request that identifies a MAC address of the gateway routing device;

updating the ARP table with the MAC address of the gateway routing device; and

identifying the MAC address in the ARP table as associated with a gateway routing device.

5. (Previously Presented) The method of Claim 2, further comprising:

determining IP addresses associated with the source MAC address in an ARP table;

determining if the IP addresses associated with the source MAC address in the ARP table are associated with a gateway routing device to determine if the source MAC address is associated with a gateway routing device; and

determining that the source IP address is not spoofed if the source MAC address is associated with a gateway routing device.

6. (Previously Presented) The method of Claim 5, wherein determining if the IP addresses associated with the source MAC address in the ARP table are associated with a gateway routing device comprises searching a routing table for the IP addresses to determine if any of the IP addresses are associated with a gateway routing device in the routing table to determine if the source MAC address is associated with a gateway routing device.

7-9. (Canceled).

10. (Currently Amended) The method of ~~Claim 1~~ Claim 2, further comprising identifying the source IP address as not bound to the source MAC address if a response is not received to the ARP request.

11. (Currently Amended) The method of ~~Claim 1~~ Claim 2, further comprising discarding the packet if no entry in the ARP table corresponding to the MAC address has an IP address which corresponds to the source IP address.

12. (Currently Amended) The method of ~~Claim 1~~ Claim 2, further comprising:

determining if the source IP address is associated with a routing device;

forwarding the packet if the source IP address is associated with a routing device; and

discarding the packet if the source IP address is not associated with a routing device and if no entry in the ARP table corresponding to the MAC address has an IP address which corresponds to the source IP address.

13-19. (Canceled).

20. (Currently Amended) The method of ~~Claim 1~~ Claim 2, further comprising discarding the packet if the source MAC address is associated with more than a predefined number of IP addresses.

21. (Original) The method of Claim 20, wherein the predefined number of IP addresses is associated with the source device.

22. (Original) The method of Claim 20, wherein the predefined number of IP addresses is associated with a subnet associated with the MAC address.

23. (Currently Amended) A method of determining if a packet has a spoofed source Internet Protocol (IP) address, comprising:

evaluating a source media access control (MAC) address of the packet and the source IP address to determine if the source IP address of the packet has been bound to the source MAC address at a source device of the packet;

determining that the source IP address of the packet is spoofed if the source IP address is not bound to the source MAC address; and

~~The method of Claim 1, further comprising~~ discarding the packet if the source IP address is associated with at least one MAC address other than the source MAC address,

wherein evaluating a source MAC address of the packet and the source IP address further comprises:

identifying an entry in an address resolution protocol (ARP) table corresponding to the source MAC address;

comparing an IP address of the identified entry to the source IP address to determine if the IP address of the identified entry corresponds to the source IP address;

identifying the source IP address as bound to the source MAC address at the source device if the IP address of the identified entry corresponds to the source IP address;

sending an ARP request to the source IP address if no entry in the ARP table is identified as corresponding to the source MAC address; and

incorporating an entry corresponding to the MAC address into the ARP table if a response is received to the ARP request.

24. (Currently Amended) The method of ~~Claim 1~~ Claim 23, further comprising forwarding the packet if the source IP address indicates that the packet is a dynamic host configuration protocol (DHCP) request.

25. (Previously Presented) The method of Claim 24, wherein forwarding the packet comprises forwarding the packet if the source IP address indicates that the packet is a dynamic host configuration protocol (DHCP) request and the contents of the packet indicate that the packet is a DHCP request.

26-28. (Canceled).

29. (Previously Presented) The method of Claim 11, further comprising logging MAC addresses of discarded packets.

30. (Currently Amended) The method of ~~Claim 1~~ Claim 23, further comprising notifying a system administrator of a subnet of the source device and the presence of a spoofed source IP address in a packet from the source device when no entry in the ARP table corresponding to the MAC address has an IP address which corresponds to the source IP address.

31. (Previously Presented) The method of Claim 11, wherein a destination device of the packet comprises a network attached storage device and wherein discarding the packet if no entry in the ARP table corresponding to the MAC address has an IP address which corresponds to the source IP address is carried out so that the packet is not forwarded to an Internet Protocol (IP) layer of the network attached storage device so as to increase the availability of the network attached storage device in the event of a denial of service attack.

32.-33. (Canceled).

34. (Currently Amended) A method of determining if a packet has a spoofed source Internet Protocol (IP) address, comprising:

evaluating a source media access control (MAC) address of the packet and the source IP address to determine if the source IP address of the packet has been bound to the source MAC address at a source device of the packet;

determining that the source IP address of the packet is spoofed if the source IP address is not bound to the source MAC address;

monitoring packets from a source device to determine if the source device has more IP addresses bound to the MAC address of the source device than a predefined limit; and

identifying the source device as having more IP addresses bound to its MAC address than the predefined limit so as to allow corrective action to be taken to reduce network degradation as a result of a denial of service attack utilizing the spoofed source IP address bound to the MAC address of the source device,

wherein evaluating a source MAC address of the packet and the source IP address further comprises:

identifying an entry in an address resolution protocol (ARP) table corresponding to the source MAC address;

comparing an IP address of the identified entry to the source IP address to determine if the IP address of the identified entry corresponds to the source IP address;

identifying the source IP address as bound to the source MAC address at the source device if the IP address of the identified entry corresponds to the source IP address;

sending an ARP request to the source IP address if no entry in the ARP table is identified as corresponding to the source MAC address; and

incorporating an entry corresponding to the MAC address into the ARP table if a response is received to the ARP request, and

wherein the corrective action to be taken to reduce network degradation as a result of a denial of service attack utilizing the spoofed source IP address bound to the MAC address of the source device comprises discarding packets from the source device and ~~The method of Claim 33, wherein the corrective action to be taken to reduce network degradation as a result of a denial of service attack utilizing the spoofed source IP address bound to the MAC address of the source device comprises~~ notifying a system administrator that the source device has more IP address bound to its MAC address than the predefined limit.

35. (Currently Amended) The method of ~~Claim 32~~ Claim 34, further comprising establishing the predefined limit based on characteristics of the source device.

36. (Currently Amended) The method of ~~Claim 32~~ Claim 34, further comprising establishing the predefined limit as a common limit for all devices on a subnet of the source device.

37. (Currently Amended) A method of determining if a packet has a spoofed source Internet Protocol (IP) address, comprising:

evaluating a source media access control (MAC) address of the packet and the source IP address to determine if the source IP address of the packet has been bound to the source MAC address at a source device of the packet;

determining that the source IP address of the packet is spoofed if the source IP address is not bound to the source MAC address;

~~The method of Claim 1, further comprising:~~

determining if a source IP address is bound to a MAC address of more than one source device; and

identifying the source devices having the IP address bound to the MAC addresses so as to allow corrective action to be taken to reduce network degradation as a result of a denial of service attack utilizing the spoofed source IP address bound to the MAC addresses of the source devices,

wherein evaluating a source MAC address of the packet and the source IP address further comprises:

identifying an entry in an address resolution protocol (ARP) table corresponding to the source MAC address;

comparing an IP address of the identified entry to the source IP address to determine if the IP address of the identified entry corresponds to the source IP address;

identifying the source IP address as bound to the source MAC address at the source device if the IP address of the identified entry corresponds to the source IP address;

sending an ARP request to the source IP address if no entry in the ARP table is identified as corresponding to the source MAC address; and

incorporating an entry corresponding to the MAC address into the ARP table if a response is received to the ARP request.

38. (Previously Presented) The method of Claim 37, wherein the corrective action to be taken to reduce network degradation as a result of a denial of service attack utilizing the spoofed source IP address bound to the MAC addresses of the source devices comprises discarding packets from the source device.

39. (Previously Presented) The method of Claim 37, wherein the corrective action to be taken to reduce network degradation as a result of a denial of service attack utilizing the spoofed source IP address bound to the MAC addresses of the source devices comprises

notifying a system administrator that the IP address is bound to MAC addresses of more than one source device.

40.-46. (Canceled).